SCIENTIFIC REPORTS

OPEN

Keyless Semi-Quantum Point-to-point Communication Protocol with Low Resource Requirements

Received: 16 April 2018
Accepted: 30 November 2018
Published online: 11 January 2019

Haoye Lu[1], Michel Barbeau[2] & Amiya Nayak[1]

Full quantum capability devices can provide secure communications, but they are challenging to make portable given the current technology. Besides, classical portable devices are unable to construct communication channels resistant to quantum computers. Hence, communication security on portable devices cannot be guaranteed. Semi-Quantum Communication (SQC) attempts to break the quandary by lowering the receiver's required quantum capability so that secure communications can be implemented on a portable device. However, all SQC protocols have low qubit efficiency and complex hardware implementations. The protocols involving quantum entanglement require linear Entanglement Preservation Time (EPT) and linear quregister size. In this paper, we propose two new keyless SQC protocols that address the aforementioned weaknesses. They are named Economic Keyless Semi-Quantum Point-to-point Communication (EKSQPC) and Rate Estimation EKSQPC (REKSQPC). They achieve theoretically constant minimal EPT and quregister size, regardless of message length. We show that the new protocols, with low overhead, can detect Measure and Replay Attacks (MRA). REKSQDC is tolerant to transmission impairments and environmental perturbations. The protocols are based on a new quantum message transmission operation termed Tele-Fetch. Like QKD, their strength depends on physical principles rather than mathematical complexity.

Two full quantum capability devices can communicate securely with Quantum Key Distribution (QKD)[1–4]. In this protocol, two communicants have to be armed with advanced quantum components including quantum registers, programmable quantum circuits and quantum generators. Most of them can only function under stable and well-configured environments and occupy large space. So, it is challenging to implement secure communications on portable devices. On the other hand, quantum computers can efficiently break RSA cryptosystem[5], the security foundation of almost all classical communication protocols. Thence, the communication security of portable devices is in imminent danger of collapse.

Semi-Quantum Communication (SQC) intends to break the predicament by limiting the quantum capability of the receiver without dampening the transmission security. The quantum components for realizing limited quantum capability can be designed compact, simple and robust so that they could be integrated into a portable device. The discussions start from two Semi-Quantum Key Distribution (SQKD) protocols reported by Boyer *et al.*[6,7]. Compared with QKD, the receiver Bob needs only to perform four quantum operations: (1) generate quantum bits (qubits) in the Z-basis, (2) measure qubits in the Z-basis, (3) permute qubits and (4) access quantum channel. These two new protocols secure the communications by randomizing measurement basis and Bob's treatment on the qubits he receives. For concealing Bob's behavior, reordering of the qubits is also required. In 2011, Jian *et al.*[8] proposed a new SQKD protocol that improves qubits efficiency (the message length with respect to the number of qubits sent by Alice) from the original 12.5% to roughly 50% by using entangled qubits. But the Entanglement Preservation Time (EPT) for implementing the protocol is at least linear to the length of the message. So is the quantum bit register (quregister) size. Li *et al.*[9] showed that Bob's quantum computation task can be delegated to a third party quantum server in semi-quantum communications at the cost of a low qubit efficiency (6.25%). In 2015, Luo and Hwang[10] proposed a new protocol showing that the Public Bidirectional Authentic Classical Channel (PBACC) is unnecessary if the two communicants have a pre-shared key. However, besides a even longer EPT and a low qubit efficiency (12.5%), a larger quregister size is required for each data bit. A similar

[1]University of Ottawa, School of Electrical Engineering and Computer Science (EECS), Ottawa, K1N 6N5, Canada. [2]Carleton University, School of Computer Science, Ottawa, K1S 5B6, Canada. Correspondence and requests for materials should be addressed to H.L. (email: hlu044@uottawa.ca)

pre-shared key based protocol proposed by Almousa and Barbeau[11] shows that Bob does not need to store any qubits, but the linear EPT persists. Recently, more work concerning SQC is reported[12–15].

All the aforementioned protocols[6–12] suffer from low qubit efficiency. Most of them have significant large linear quregister size overhead and require permutation of qubits[6–8,10,11]. Regarding the protocol involving entangled qubits[8,10,11], the quantum EPT is at least linear. Although a six-hour record has been achieved by Zhong *et al*. utilizing europium ion implanted in a crystal[16], entanglement time declines considerably should the entangled photons be propagated in an optical fiber (the most common implementation of quantum communication protocols)[17]. Besides, involving permutations on qubits (not practical shortly) dooms to a low transmission efficiency and reliability. Considering that the unusual materials (for instance, coupled electron[18] and ultracold atoms[19]) are necessary for the implementation of quregisters, a commercial quantum network based on them is not feasible in a near future.

This paper reports a new Semi-Quantum Direct Communication (SQDC) protocol and a rate estimation version, named Economic Keyless Semi-Quantum Point-to-Point Communication (EKSQPC) and Rate Estimation EKSQPC (REKSQPC), that address all the aforementioned issues. An innovative operation, called Tele-Fetch (TF), utilizes entangled qubit pairs to transmit messages. It is at the core of the One-Bit Protocol (OBP). The results of measurements on the pairs fall in a predesigned set of values because of the entanglement, but do not carry any useful information. The design makes the OBP functioning without a pre-shared key and fully resistant to information leakage even if the qubits are intercepted. Besides, the protocol uses the same quantum circuit as the one to detect the Measure and Replay Attack (MRA) (called MRA Detection (MRAD)) and thus, not only saves the quantum resources but also becomes the cornerstone of the EKSQPC and REKSQPC protocols. Because Alice performs the same quantum procedures in both protocols (OBP or MRAD), Bob does not need to communicate with Alice until all quantum procedures (Alice's and Bob's) are completed. Alice and Bob execute MRADs using a small portion of the measurement results before using the PBACC to translate the rest into valid messages. The protocol is proved fully secure under the assumption that MRA are always detectable. As the pivot to secure the messages is a successful detection of MRA, we show that, with only 15 probing bits, the attack detection success rate can achieve 0.995 (under the assumption that the adversary Eve has 0.6 possibility to attack a qubit). The security of the protocol is enhanced considerably if a few more probing bits are added. The qubit efficiency asymptotically reaches 100% with the message length. The implementation of the EKSQPC protocol has low requirements on quantum resources. In particular, the quregister size required by Alice is as low as one, and the required EPT is $C+2T$ (where C is the time that Alice takes to generate, send and receive the qubits; and T is the one-way time for the qubits to travel between Alice and Bob). We prove that both the quregister size and EPT reach the theoretical minimums.

Considering that the entanglement of qubits may not always persist during the transmission of qubits, we assume that there is a probability ω that the entanglement involving a qubit is destroyed as it can be disturbed by hardware imperfection and environmental disturbance. Under this assumption, we design a statistical test to compare ω with the probability that a qubit is attacked or disturbed. When a significant difference is observed, Alice concludes that Eve perpetrated attacks and aborts the execution of the protocol. Therefore, the communication is not eavesdropped successfully. Compared with the original EKSQPC, more probing bits are required to achieve the same detection success rate; however, the overhead is still low. In particular, our simulation results reveal that 60 probing bits are enough to detect almost all attacks when ω is unknown. If the rate is given, then 40 probing bits are enough to achieve the same detection success rate.

This paper is a revised and extended version of a preliminary workshop paper[20] in which we introduced the original EKSQPC protocol. Compared to the workshop paper, this paper articulates the original protocol as well as its analysis with more details. Based on this, we report an upgraded and practical version, REKSQPC, with its security, resource requirements and transmission efficiency analysis. Moreover, we also provide a detailed comparison with other typical SQKD and SQDC protocols.

The rest of the paper is organized as follows. In Section 2, we review Bell measurement and MRAD, which are integrated in the new protocol. In Sections 3 and 4, we introduce our new protocols including a rate estimation version taking into account the probability that a qubit is disturbed. We also do a security analysis and discuss simulation results. In Section 5, we talk about their quantum resource requirements and transmission overhead. Finally, we draw the conclusions in Section 6.

Background

The section starts from a brief review of EPR pairs states and Bell measurement on which our new protocol heavily relies. Then we introduce the MRA as well as its detection algorithm (MRAD) that secures the data transmission of the new protocol.

In this paper, classical bits (cbits) are denoted by lowercase English letters, and a cbit sequence is represented by an uppercase English letter over a tilde. For instance, $\underset{\sim}{M} = m_1 m_2 \cdots m_t$ is a cbit string of length t. Qubits are denoted by Greek letters and Bell states by Bold English capital letters.

EPR pairs and Bell measurement. A pair of qubits that are together in Bell state is called an EPR pair. Bell states have four types: $|\Phi^+\rangle = \frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle)$, $|\Phi^-\rangle = \frac{1}{\sqrt{2}} \cdot (|00\rangle - |11\rangle)$, $|\Psi^+\rangle = \frac{1}{\sqrt{2}} \cdot (|01\rangle + |10\rangle)$, and $|\Psi^-\rangle = \frac{1}{\sqrt{2}} \cdot (|01\rangle - |10\rangle)$; we can use the Bell measurement (B.M.) (Fig. 1) to identify them. The inputs of the circuit are two qubits γ_A and γ_B, and the outputs are two cbits e_1 and e_2.

If $\gamma_A\gamma_B$ is an EPR Pair (Bell state), then the outputs are deterministic and listed in Table 1; otherwise, $\gamma_A\gamma_B$ is mapped into a Bell state stochastically. For $\gamma_A\gamma_B$ equal to $|00\rangle, |01\rangle, |10\rangle$ or $|11\rangle$, the distributions of the outputs are listed in Table 2.

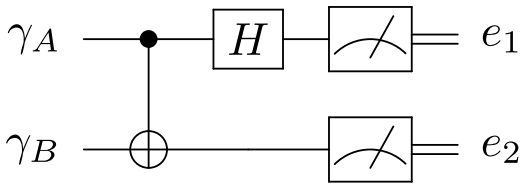

Figure 1. The Bell measurement Circuit.

$\gamma_A\gamma_B$	Output (e_1e_2)	$\gamma_A\gamma_B$	Output (e_1e_2)
$\|\Phi^+\rangle$	00	$\|\Phi^-\rangle$	10
$\|\Psi^+\rangle$	01	$\|\Psi^-\rangle$	11

Table 1. Bell measurements on Bell states.

$\gamma_A\gamma_B$	Output (e_1e_2)	$\gamma_A\gamma_B$	Output (e_1e_2)
$\|00\rangle$	00	$\|01\rangle$	01
	10		11
$\|10\rangle$	01	$\|11\rangle$	00
	11		10

Table 2. Bell measurement results of $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$; there is 0.5 possibility for each output.

Measure and Replay Attack and the method of detection. A simplified version of Man-In-The-Middle Attacks (MITMs) is called replay attack. The attacker Eve deceives the truthful listener(s) by replaying messages outside the expected context so that the listener believes that the protocol has been executed successfully[21].

We can perpetrate a similar attack in the context of quantum communications. Assume that qubits sent or received by Alice and Bob can be intercepted by Eve. As a qubit is sent to Bob by Alice through the quantum channel, Eve uses the Z-basis to measure it. If the measurement result is zero, then Eve sends $|0\rangle$ to Bob; otherwise, she sends $|1\rangle$. As the replay of the message follows the measurement, we call the attack the Measure and Replay Attack (MRA)[11].

The following method demonstrates how to utilize the EPR pairs and Bell measurement to detect MRA. The Luo and Hwang's protocol[10] and Almousa and Barbeau's protocol[11] also apply similar ideas for the attack detection.

MRA Detection (MRAD):

D1 Alice randomly picks a cbit $i = 0$ or 1, based on which she generates an EPR pair $\mathbb{E}$ (if $i = 0$, $\mathbb{E} = |\Phi^+\rangle$; else, $\mathbb{E} = |\Psi^-\rangle$).

D2 $\mathbb{E}$ consists of two qubits, γ_A and γ_B. Alice keeps γ_A and sends γ_B (named the probing bit) to Bob.

D3 γ_B is reflected by Bob to Alice.

D4 After receiving γ'_B, Alice applies Bell measurement (Fig. 1) on $\gamma_A\gamma'_B$ to obtain e_1 and e_2.

D5 The combination of e_1 and e_2 indicates the EPR pair that the circuit measured. We consider the protocol secure (denoted by zero) if the measured EPR pair agrees with the one Alice produced in Step D1. If not, an MRA is detected (denoted by one).

Example 1. *Suppose Alice and Bob implement* MRAD *for* MRA *detection. Without loss of generality, assume Alice picks* $i = 1$ *and thus produces a corresponding EPR pair* $\mathbb{E} = |\Psi^-\rangle = \frac{1}{\sqrt{2}} \cdot (|01\rangle - |10\rangle) = \gamma_A\gamma_B$. *Alice intends to send* γ_B *to Bob; however, Eve intercepts and measures it and gets the measurement result* $r = 0$. *Simultaneously,* γ_A *retained by Alice collapses to* $|1\rangle$ *due to the entanglement. Eve produces a new qubit* ($|0\rangle$) *correspondingly and send it to Bob. Bob does nothing but reflects it back to Alice.* γ_A *and the received* $|0\rangle$ *are paired together and measured by Alice using the Bell measurement circuit. Notice that* γ_A *has collapsed to* $|1\rangle$. *So the qubit pair measured by the circuit is* $\gamma_A\gamma_B = |10\rangle$. *By* Table 2, *we have* 50 *percent possibility to get* $e_1e_2 = 01$ (*and so deduce that the input is* $|\Psi^+\rangle$ *by* Table 1, *a true positive*) *and to get* $e_1e_2 = 11$ (*and thus deduce that the input is* $|\Psi^-\rangle$, *a false negative*).

The example shows that if Alice picks $i = 1$ and the measurement result r of Eve is zero, there is 50 percent possibility for Alice to deduce that the protocol is secure although the attack is perpetrated. By Table 2, we can draw the same conclusion for any choice of i and r. Hence, Lemma 1 and Theorem 1 follow.

Lemma 1. *Provided that Eve attacks the probing bit, there is* 0.5 *possibility for MRAD to detect an MRA.*

Theorem 1. *If MRAD are repeated n times, we have* $1-0.5^n$ *probability to detect MRA given that Eve attacks n probing bits.*

Proof. $Pr[\text{detect MRAs}]=1-Pr[\text{MRAD fails}]^n=1-0.5^n\square$

Remark 1. *MRAD essentially checks whether the probing bits sent by Alice had been measured by anybody else, but it cannot tell who measured them. It can detect MRA only because Alice knows that Bob does not measure probing bits. Therefore, if any measurement is detected, it must be due to an attack.*

Because, the operations defined in Steps D1 and D5 are applied again in the sequel, we define them formally as follows,

Definition 1 (Generating corresponding EPR pairs (*F*), Step D1). *Function F maps a* cbit *to an EPR pair such that* $0 \mapsto |\Phi^+\rangle$, and $1 \mapsto |\Psi^-\rangle$

Definition 2 (Alice Examines (AE), Step D5). *The function* $AE(e_1, e_2, i)$: $\{0, 1\}^3 \rightarrow \{0, 1\}$ *equals zero if* $e_1 = e_2 = i$; *otherwise, it equals one. Recall that zero and one indicate negative and positive detection results, respectively.*

New Protocol

In this section, we propose a new SQDC protocol called EKSQPC. We start the discussion with an introduction to a data transmission protocol called OBP, which is a building block of EKSQPC (not self-contained). Assuming that there are no MRA, we show that OBP is secure (Theorem 2). In the design of OBP, Bell measurement seems redundant. It is intended for sharing the quantum circuit with MRAD (Remark 2). The considerable benefits of this design are discussed in Section 5. To meet the assumption of Theorem 2, we integrate MRAD and OBP to get EKSQPC. If we assume that EKSQPC detects all MRA, then it is provably secure (Theorem 4).

One-Bit Protocol (OBP)

Protocol 1 (OBP): *A one-bit message m* **(***zero or one***)** *is sent to Bob by Alice.* **(***PBQC***).** *The protocol functions as follows***:**

P1. *Alice randomly picks a cbit i and generates a corresponding EPR pair* $\mathbb{E} = F(i)$ *(Definition 1) consisting of two qubits (denoted by* γ_A *and* γ_B*).*
P2. *Alice keeps* γ_A *and sends* γ_B *to Bob.*
P3. *Upon reception, the qubit* γ_B *is measured by Bob in the Z-basis with the measurement result* u_B *(simultaneously,* γ_A *collapses because of the entanglement with* γ_B*). At the same moment, Bob sends a pre-prepared qubit* $\gamma_B^* = 0$ *to Alice and informs her that he has measured* γ_B *via the PBACC.*
P4. *Alice pairs* γ_A *(retained in Step P1) with* γ'_B *and performs a Bell measurement on* $\gamma_A\gamma_B^* = \gamma_A|0\rangle$ *to get* e_1 *and* e_2*.*
P5. *According to* Table 2, $e_1e_2 = 00$ *or* 10 *implies that* $\gamma_A = |0\rangle$*, and* $e_1e_2 = 01$ *or* 11 *indicates that* $\gamma_A = |1\rangle$*. Combining* γ_A *with the EPR pair* $\mathbb{E}$ *Alice selected (recorded by i) in Step P1, Alice learns the measurement result* u_B *of Bob in Step P3. In particular, if* $i = 0$*, then the EPR pair she generated was* $|\Phi^+\rangle$*. Then* $\gamma_A = |0\rangle$ *implies* $u_B = 0$*, and* $\gamma_A = |1\rangle$ *implies* $u_B = 1$*. Similarly, if* $i = 1$*, the EPR pair that Alice generated was* $|\Psi^-\rangle$*. Then if* $\gamma_A = |0\rangle$*,* $u_B = 1$*; else,* $u_B = 0$*.*
P6. *Provided that* $u_B = m$*, Alice informs Bob, via the PBACC, that* u_B *is the correct value. Otherwise, she informs Bob to take* $1 - u_B$*.*

Remark 2. *The pre-generated* qubit $\gamma_B^* = 0$ *in Step P3 is unnecessary to implement* OBP*. So is the Bell measurement in Step P4. In fact, in Step P3, Bob only needs to notify Alice that he has measured* γ_B*, and, in Step P4, Alice simply uses the Z-basis to get the value of* γ_A*. Here, we intendedly implement OBP with redundant operations so that the new protocol (EKSQPC, introduced in Section 3.2) can use a single quantum circuit to implement both the attack detection (MRAD) and data transmission (OBP) protocols. We discuss the design and its benefits in details in Section 3.2, and more performance analysis is conducted in Section 5.*

The actions specified in Steps P5 and P6 are used subsequently. We define them formally as follows. In Step P5, Alice learns r_B held by Bob with no contact. So the function is called Tele-Fetch.

Definition 3 (Tele-Fetch). *With the parameters* e_1, e_2 *and i (Step P1), function Tele-Fetch* $TF(e_1, e_2, i)$ *returns the value of* r_B *(zero or one) based on the rule contained in Step P5.*

Besides, in Step P6, Alice rectifies the measurement result r_B of Bob. As a result, we call the procedure Rectify.

Procedure 1 (Rectify). *Based on the single bit message m and value of* u_B *(acquired in Step P5), Alice informs Bob to apply the proper operation on* u_B *by sending either the signal KEEP or FLIP via the PBACC. If KEEP is received, Bob considers* u_B *as the message Alice sends; if not, he takes* $1 - u_B$*.*

The next theorem discusses the security of OBP.

Theorem 2. *As long as Bob gets the qubit* γ_B *sent by Alice without MRA, OBP is secure.*

Proof. By assuming the absence of MRA, we essentially assume that Steps P1 to P3 are secure (only a confirmation is sent by Bob in Step P3). No communication happens in Step P4 and P5. The last step involves a message sent by Alice which is irrelevant to the one-bit message m. So Step P6 is sheltered, too. Thence, to sum up, OBP is secure.□

Remark 3. *An authentic classical channel is the prerequisite for the security of OBP. In the communication of Alice and Bob, it is significant to verify their identities and to ensure that their unencrypted messages are not altered. Namely, they should be resistant to MITMs.*

Theorem 2 shows that only when there is no MRA, OBP is secure. However, OBP has no capability to detect MRAs. Notice that MRAD can detect MRAs and thus can secure the data transmission of OBP by Theorem 2. If we combine OBP and MRAD together, we get the protocol discussed in the following subsection.

Economic Keyless Semi-Quantum Point-to-Point Communication (EKSQPC). We implement the protocol EKSQPC over the hardware of OBP. Specifically, there are a PBACC and a PBQC linking Alice and Bob. The following four procedures contain all the activities demanding quantum resources in EKSQPC.

Procedure 2 (Alice sends). *In the k^{th} transmission of Alice, she picks a random* cbit i_k*and stores it in a classical register. Then she produces an EPR pair $F(i_k)$, keeps the first qubit γ_{kA} and transmits the second qubit γ_{kB} to Bob.*

Procedure 3 (Bob measures). *After receiving the k^{th} qubit from Alice, Bob measures it in the Z-basis and gets the result u_k. At the same moment, a pre-prepared qubit $|0\rangle$ is sent back to Alice. Furthermore, Bob takes the record that he measured the k^{th} qubit.*

Procedure 4 (Bob reflects). *The k^{th} qubit from Alice is reflected back without measurement by Bob. Also, he takes the record that he reflected the k^{th} qubit he received.*

Procedure 5 (Alice measures). *Alice receives the k^{th} qubit γ_{kB}^{*} and performs Bell measurement on $\gamma_{kA}\gamma_{kB}^{*}$ (γ_{kA} was retained by Alice in Step C1 while implementing Procedure 2) and records the measurement result as $e_{1k}e_{2k}$.*

Protocol 2 (EKSQPC): *Assume that a message $\underset{\sim}{M} = m_1m_2\cdots m_s$ of length s is sent to Bob by Alice, and extra r bits are added to detect* MRA. *Then the protocol functions as follows*:

C1. *Alice runs Procedure 2 for $s + r$ times and records the values of i_k in string $\underset{\sim}{I} = i_1i_2\cdots i_{s+r}$.*
C2. *Bob randomly selects s qubits (data bits) from the $s + r$ qubits that Alice sends to implement Procedure 3. Regarding the residual r qubits (probing bits), he executes Procedure 4. All the measurement results u_k from Procedure 3 are recorded in a new string $\underset{\sim}{U} = u_1u_2\cdots u_s$ (after reindexing but preserving the order).*
C3. *Alice performs Procedure 5 on the $s + r$ qubits that Bob sends back, and records the measurement results $e_{1k}e_{2k}$ in two strings $\underset{\sim}{E}_1 = e_{11}e_{12}\cdots e_{1(s+r)}$ and $\underset{\sim}{E}_2 = e_{21}e_{22}\cdots e_{2(s+r)}$, respectively.*
C4. *Bob sends a binary string $\underset{\sim}{P} = p_1p_2\cdots p_{s+r}$ to Alice through the PBACC to inform her about which qubits were reflected or measured in Step C2. For $k = 1, 2, \cdots, s + r$, $p_k = 0$ indicates that Bob reflected the k^{th} qubits, and $p_k = 0$ represents he measured it.*
C5. *Alice iterates through $\underset{\sim}{P}$ sent by Bob. For $k = 1, 2, \ldots, s + r$, when $p_k = 0$, Alice applies function $AE(e_{1k}, e_{2k}, i_k)$ in Definition 2. If $AE(e_{1k}, e_{2k}, i_k) = 1$, then the k^{th} qubits sent by Alice is attacked by Eve (MRA). Then the protocol is insecure and terminated. While if $p_k = 1$, Alice evaluates function $TF(e_{1k}, e_{2k}, i_k)$ in Definition 3 and records the value c_k. Remark that, before reindexing, c_k coincides with u_k in Step C2.*
C6. *Since s qubits are measured by Bob, Alice applies function TF s times in Step C5. She records the values of c_k in $\underset{\sim}{C} = c_1c_2\cdots c_s$ (after reindexing without altering the order). Note that $\underset{\sim}{C}$ coincides with $\underset{\sim}{U}$ that is owned by Bob.*
C7. *Alice and Bob execute Procedure 1 with patemeters m_k, c_k and u_k ($k = 1, 2, \ldots, s$). Then Bob receives the message sent by Alice.*

Remarkably, Alice and Bob implement Steps C1 to C3 in parallel rather than sequentially. As a result, Alice is only required to be equipped with a small and fixed number of quregisters. Also, the time for Alice to keep the entanglement is a small constant irrelevant to the message length (we elaborate on this highlight in Section 5.1). The protocol essentially distributes a random string of length m between Alice and Bob, which implies that our protocol is also a SQKD protocol. After sharing a binary string, Bob can receive messages from Alice by implementing Procedure 1. To mitigate the cost of sharing keys, Step C7 can be repeated for several message transmissions before adopting a new shared string $\underset{\sim}{U}$ ($= \underset{\sim}{C}$) (by repeating Steps C1 to C6).

The EKSQPC protocol is an integration of OBP and MRAD. Fig. 2 demonstrates that, in the first four steps, the operations belonging to Alice coincide. Notice that these four steps include all the operations of OBP and MRAD that require quantum resources. As a result, without knowledge of the protocol she is in fact executing, Alice can use one quantum circuit to accomplish all the quantum operations required by either of the protocols.

In Fig. 2, we juxtapose the first four steps of OBP and MRAD marked with the step numbers used to present them. On the right, the step numbers used in the EKSQPC protocol are also provided.

From Fig. 2, only the operation made by Bob differentiates OBP from MRAD. Namely, Bob decides which protocol is being implemented. Specifically, to decide the protocol being applied, Bob either measures γ_{kB} (and

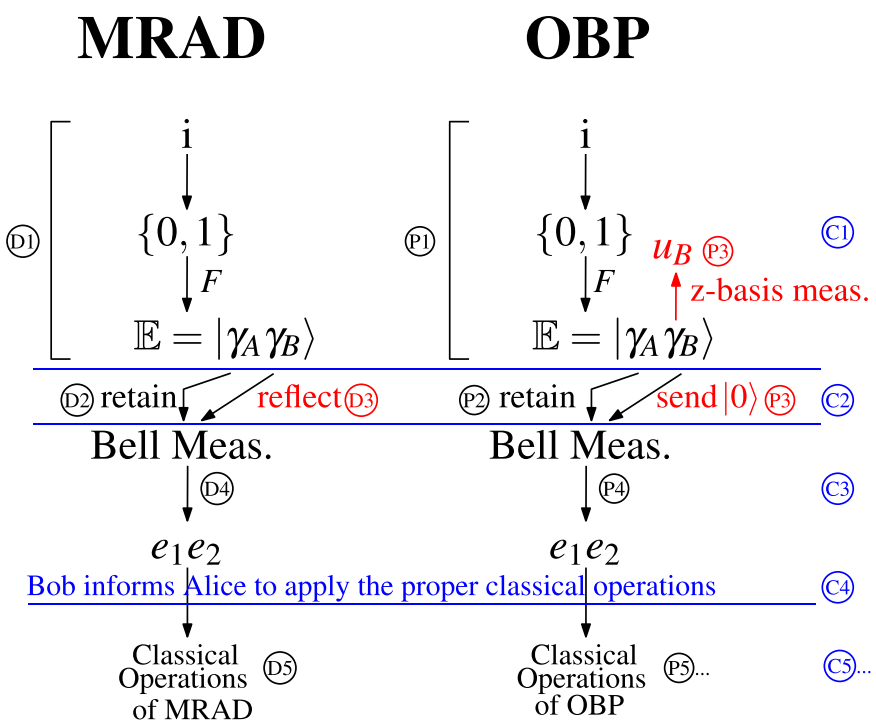

Figure 2. The relationships between EKSQPC, OBP and MRAD. The actions in red are made by Bob and those in Black are performed by Alice. The step numbers in blue are the corresponding actions in EKSQPC. In OBP and MRAD, quantum operations (first four steps) are quite similar except Bob's treatment on the qubits sent by Alice.

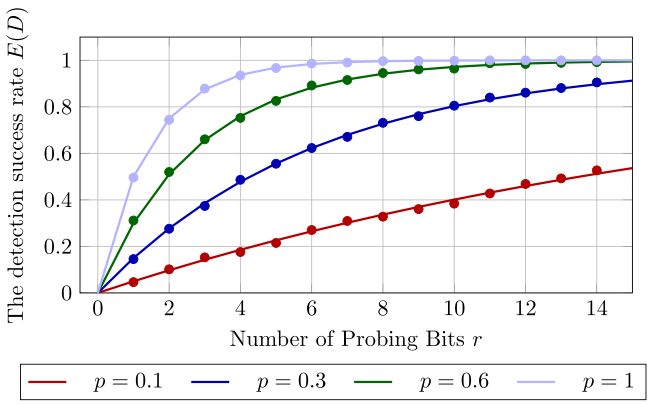

Figure 3. The detection success rate $E(D)$ with respect to the probing bit number r by selecting various attack probability p.

send a pre-prepared $|0\rangle$ simultaneously) or reflects it. Note that the pre-preparation of the $|0\rangle$, instead of generating it on demand, secures EKSQPC against the delay and reflection attacks[11]. A reflected γ_{kB} functions as a probing bit to detect MRA (then Alice and Bob implement MRAD), and a measured γ_{kB} works as a data bit for data exchange (then Alice and Bob implement OBP). After completing the first three steps of EKSQPC, Bob informs Alice of the qubits reflected or measured by sending a notification through the PBACC. Based on the message, Alice applies the corresponding classical operations to complete MRADs or OBPs.

Remark 4. *The protocol being implemented is determined by Bob. If Bob chooses Measure, then it is OBP. If he chooses Reflect, then it is MRAD. In EKSQPC, Bob selects Measure s times and Reflect r times. So Alice and Bob execute OBP s times and MRAD r times.*

Security analysis of EKSQPC. The EKSQPC inherits the security of OBP and functions under the same assumption – Alice and Bob must be connected by an authentic classical channel (Remark 3). By Remark 4, EKSQPC with s data bits and r probing bits is equivalent to s OBPS and r MRADs. Recall that MRAD is for

detecting MRA and thus secures OBP (Theorem 2). When MRADs are performed n times, the possibility of detecting MRA is $1-0.5^n$ (Theorem 1). In particular, since there are r times executions of MRADs in the EKSQPC protocol, we have $1-0.5^r$ success rate of detection given that all qubits sent by Alice are measured by Eve. If we generalize the problem by assuming that Eve perpetrates MRA on the qubits with a fixed probability, we have the theorem as follows.

Theorem 3. *Suppose that Alice and Bob implement the EKSQPC protocol with s data bits and r probing bits. For each qubits sent by Alice, if Eve has probability p to perpetrate MRA, then Alice has the probability* $1-(1-p/2)^r$ *to detect it.*

Proof. Let A be the number of probing bits attacked by Eve. As Eve has possibility p to perpetrate an MRA on each probing bit, A follows a binomial distribution having success rate p with r trials. Let D be a boolean Random Variable (r.v.) such that $D=1$ if Alice detects an attack and $D=0$ if not. Then the expectation $E(D)$ is the probability of detecting an attack, and it satisfies

$$\begin{aligned}
E[D] &= 0\cdot Pr[D=0]+1\cdot Pr[D=1]\\
&= Pr[D=1]\\
&= \sum_{h=0}^{r} Pr[D=1|A=h]Pr[A=h] \quad \text{(Law of total probability)}\\
&= \sum_{h=0}^{r}(1-0.5^h)\binom{r}{h}p^h(1-p)^{r-h} \quad \text{(by Theorem 1)}\\
&= \sum_{h=0}^{r}\binom{r}{h}p^h(1-p)^{r-h}\\
&\quad -\sum_{h=0}^{r}0.5^h\binom{r}{h}p^h(1-p)^{r-h}\\
&= 1-(0.5p+(1-p))^r \quad \text{(Binomial expansion)}\\
&= 1-(1-0.5p)^r
\end{aligned}$$

□

Regarding Theorem 3, if $p=1$, Eve attacks all the qubits that Alice sends. Then the probability of detecting an MRA is $E(D)=1-(1-0.5)^r=1-0.5^r$, which is consistent with the discussion at the beginning of Section 3.3.

Fig. 3 plots the trend of the detection success rate, calculated according to the formula stated in Theorem 3. We also scatter the experimental results (the points) from simulation. According to what the legend shows, the points and curves colored the same share the same attack probability p. The results of the simulation agree with the theoretical analysis in Theorem 3. The figure shows that the detection success rate approaches to one more rapidly as p increases. This trend is due to the fact that a higher attack rate leads to a higher average number of affected probing bits and thus boosts the detection success rate. A similar trend can be observed if the probing bit number r increases.

The next theorem shows the EKSQPC protocol is secure under the assumption that we can always detect MRA.

Theorem 4. *The EKSQPC protocol is secure if MRA can always be detected.*

Proof. Alice and Bob terminate the protocol if an MRA is detected. So the security of the message is guaranteed. Otherwise, there is no attack because of the assumption. According to Remark 4, the EKSQPC protocol with s data bits performs OBP for s times. Combining with Theorem 2, we conclude that the EKSQPC protocol is resistant to any network attack.

Remark 5. *It is the prerequisite for Theorem 4 that only one qubit is involved when Alice and Bob send, measure or reflect* qubits. *This implies that the implementation of the protocol requires a generator of an individual photon stream which is, however, currently not available. In practice, if we use weak laser pulses out of expediency, more than one photon may be included. This enables Photon Number Splitting (PNS) attacks which cannot be handled by our protocol. To avoid the attacks related to PNS, readers may refer to Refs*[22–25]. *The same comment also applies to Theorem 7.*

Rate Estimation EKSQPC (REKSQPC)

EKSQPC detects MRA and is secure assuming no hardware fault nor environmental disturbance that destroy entanglement. So far, we ignored them for the sake of simplicity. They do exist in practice. Ignoring them produces false positives and incorrect protocol terminations. In this section, we enhance the detection part of the protocol to fix this issue. Destructions of entanglement involving probing bits may result in Positive MRADs (PMs) whose probability is denoted by ρ and estimated by its rate

$$\hat{\rho} := \frac{\text{Number of PMs}}{\text{Number of probing bits}}.$$

The destructions have two types. In particular, we say that a qubit is disturbed if the entanglement involving it is destroyed due to a hardware imperfection or an environmental disturbance. If the destruction of the entanglement is caused by an eavesdropper Eve, we say the qubit is attacked. We show that two times $\hat{\rho}$ is an estimator $\hat{\kappa}$ of the probability κ that a probing bit is disturbed or attacked. Let ω denote the probability that a qubit is disturbed. If ω is unknown, we can estimate it ahead of the protocol execution assuming that Eve does not perpetrate attacks. As no qubits are attacked during the estimation, κ is reduced to ω. Correspondingly, $\hat{\kappa}$ is reduced to $\hat{\omega}$, an estimator of ω. During the execution of the protocol, the attacks perpetrated by Eve increase κ and cause its deviation from ω. By monitoring the difference between κ and ω, we gauge the existence of attacks and thus the security of the protocol. We use the following symbols and facts for the statistical analysis in the sequel. Let $B(n, p)$ be a binomial distribution with $n \in \mathbb{N}$ trials and success rate $p \in [0, 1]$, $N(\mu, \sigma^2)$ be a normal distribution with mean $\mu \in \mathbb{R}$ and variance σ^2 and $\overline{X}$ be the arithmetic mean of X.

Remark 6. *We call $B(1, p)$ a Bernoulli distribution with the success rate p.*

Remark 7. *r.v. of binomial distributions can be added if they have the same success rate. In particular, if $X \sim B(n, p)$ and $Y \sim B(m, p)$, then $X + Y \sim B(n + m, p)$*[26].

Fact 1. *Suppose $X \sim N(\mu_X, \sigma_X^2)$. Then $\frac{X-\mu_X}{\sigma_X}$ follows a standard normal distribution. Namely, $\frac{X-\mu_X}{\sigma_X} \sim N(0, 1)$.*

Fact 2. *Suppose $X \sim N(\mu_X, \sigma_X^2)$ and $n \in \mathbb{R}^+$. Then, $\frac{X}{n} \sim N\left(\frac{\mu_X}{n}, \frac{\sigma_X^2}{n^2}\right)$.*

Fact 3. *Suppose $X \sim N(\mu_X, \sigma_X^2)$ and $Y \sim N(\mu_Y, \sigma_Y^2)$ are independent. Then, $X - Y \sim N(\mu_X - \mu_Y, \sigma_X^2 + \sigma_Y^2)$.*

Theorem 5 discusses the random processes in the detection of disturbed and attacked qubits.

Theorem 5. *Suppose that in the* EKSQPC *protocol, Bob reflects r qubits. Let $D_i \in \{0, 1\}$ denote a r.v. of the detection result d_i of the i^{th} MRAD such that*:

$$d_i = \begin{cases} 1 & \text{if the } i^{th} \text{ MRAD has a positive detection result} \\ 0 & \text{otherwise} \end{cases}$$

Then D_i's are independent and identically distributed (iid) $B(1, \rho)$. Or in short, $D_i \overset{iid}{\sim} B(1, \rho)$. The number of PMs (denoted by C_ρ) is $\sum_{i=1}^{r} D_i$, which is a binomial distribution $B(r, \rho)$. Moreover, $\rho = \kappa/2$.

Proof. Since ρ is the probability of positive detection and all MRADs are mutually independent, $D_i \overset{iid}{\sim} B(1, \rho)$ for $i = 1 \cdots r$. Then the number of PMs $C_\rho = \sum_{i=1}^{n} D_i$. By Remark 7, we have $C_\rho \sim B(r, \rho)$. Let A_i be a r.v. such that, if the probing bit of i^{th} MRAD is disturbed or attacked, then $A_i = 1$; otherwise, $A_i = 0$. So we have, $Pr[A_i = 0] = 1 - \kappa$ and $Pr[A_i = 1] = \kappa$. According to Lemma 1, if the probing bit is disturbed or attacked, the probability of a positive detection is $Pr[D_i = 1|A_i = 1] = \frac{1}{2}$. Otherwise, the probing bit is intact which implies that the result must be negative. Namely, $Pr[D_i = 1|A_i = 0] = 0$. By Law of total probability,

$$\begin{aligned} \rho &= Pr[D_i = 1] = Pr[D_i = 1|A_i = 1] \\ &\quad \cdot Pr[A_i = 1] + Pr[D_i = 1|A_i = 0] \\ &\quad \cdot Pr[A_i = 0] = \frac{1}{2} \cdot \kappa + 0 \cdot (1 - \kappa) = \frac{\kappa}{2}. \end{aligned}$$

□

Remark 8. *A binomial distribution $B(n, p)$ has mean np and variance $np(1 - p)$. So the binomial distribution $C_\rho \sim B(r, \rho)$ in Theorem 5 has mean $r\rho = \frac{\kappa}{2}r$ and variance $r\rho(1 - \rho) = \frac{1}{2}r\kappa\left(1 - \frac{\kappa}{2}\right)$*[26].

Remark 9. *A binomial distribution $B(n, p)$ can be approximated by a normal distribution with the same mean and variance if $n \geq max\left\{\frac{45(1-2p)^2}{p(1-p)}, \frac{14 \mid 1-6p(1-p)\mid}{p(1-p)}\right\}$*[27]. *Therefore, the binomial distribution $C_\rho \sim B\left(r, \frac{\kappa}{2}\right)$ in Theorem 5 has a normal approximation $N(\frac{\kappa}{2}r, \frac{1}{2}\kappa r(1 - \frac{\kappa}{2}))$ if $r \geq max\left\{\frac{180(1-\kappa)^2}{p(2-\kappa)}, \frac{56 \mid 1-3\kappa(1-0.5\kappa)\mid}{\kappa(2-\kappa)}\right\}$.*

Theorem 6 provides a method to estimate the parameter p of a Bernoulli distribution[26].

Theorem 6. *Suppose that $X_i \overset{iid}{\sim} B(1, p)$ for $i \in \{1, 2, \ldots, n\}$. Then $\hat{p} = \overline{X} = \frac{\sum_{i=1}^{n} x_i}{n}$, is an unbiased estimator of p.*

By Theorem 6, $\rho = \frac{\kappa}{2}$ has an unbiased estimator $\hat{\rho} = \widehat{\kappa/2} = \frac{\sum_{i=1}^{r} D_i}{r} = \frac{C_\rho}{r}$. Therefore, κ can be estimated by

$$\hat{\kappa} = \frac{2C_\rho}{r}. \tag{1}$$

Remark 9 states that $C_\rho = \sum_{i=1}^{r} D_i \sim B\left(r, \frac{\kappa}{2}\right)$ approximately follows the normal distribution $N(\frac{\kappa r}{2}, \frac{1}{2}\kappa r(1 - \frac{\kappa}{2}))$. Combining with Fact 2, we conclude that $\widehat{\kappa/2} = \frac{C_\rho}{r} \sim N\left(\frac{\kappa}{2}, \frac{\kappa\left(1-\frac{\kappa}{2}\right)}{2r}\right)$. Applying Fact 2 again, we have $\hat{\kappa} \sim N\left(\kappa, \frac{2\kappa\left(1-\frac{\kappa}{2}\right)}{r}\right)$.

Rate difference monitoring. When ω is unknown, we need to estimate it before starting the execution of the protocol. We have to assume that during this estimation, there is no attack. Under this assumption, κ is reduced to ω, the probability that a probing bit is disturbed. Correspondingly, $\hat{\kappa}$ is reduced to an estimator of ω. Namely, $\kappa = \omega$ and $\hat{\kappa} = \hat{\omega}$. As we have shown $\hat{\kappa} \sim N\left(\kappa, \frac{2\kappa\left(1-\frac{\kappa}{2}\right)}{r}\right)$, we also have $\hat{\omega} \sim N\left(\omega, \frac{2\omega\left(1-\frac{\omega}{2}\right)}{s}\right)$, where s is the number of probing bits for estimating ω. Let $C_\rho^{'}$ denote the number of PMs under the assumption that the probing bits are not attacked. By replacing C_ρ by $C_\rho^{'}$ and s by r in Equation (1), we get,

$$\hat{\omega} = \frac{2C_\rho^{'}}{s}. \tag{2}$$

In REKSQPC, the attack detection method is implemented by checking that $\kappa = \omega$. After getting the estimations of κ and ω, let e denote their difference, which is an outcome of r.v. $E = \hat{\kappa} - \hat{\omega}$. Fact 3 states that E still follows a normal distribution. In particular, $E \sim N\left(\kappa - \omega, \frac{2\kappa\left(1-\frac{\kappa}{2}\right)}{r} + \frac{2\omega\left(1-\frac{\omega}{2}\right)}{s}\right)$. Under the null hypothesis H_0 that there is no attack, $\kappa = \omega$. Then $E \sim N\left(0, 2\nu\left(1 - \frac{1}{2}\nu\right)\left(\frac{1}{r} + \frac{1}{s}\right)\right)$, where $\nu = \kappa = \omega$ and can be estimated by $\hat{\nu} = \frac{2(C_\rho^{'} + C_\rho)}{r+s}$. So, if H_0 is true, the distribution of r.v. E is condensed near zero. Although the set of the possible outcomes of E is $\mathbb{R}$, the test can rule out outcomes that are much greater than zero without introducing much error (note that we do not consider a negative difference because κ is, theoretically, not less than ω. In other words, the alternative hypothesis H_1 is $\kappa > \omega$). Let α denote the probability that an outcome of E is much greater than zero and ruled out by the test. We can test H_0 against H_1 by rejecting H_0 if we observe an outcome of E greater than e_α, where $e_\alpha \in \mathbb{R}$ such that $Pr[E > e_\alpha] = \alpha$. In other words, the protocol is considered insecure if e, the difference between the estimations of κ and ω, is greater than e_α.

The arduous calculation of e_α can be avoided if we scale E to

$$Z = \frac{E - 0}{\sqrt{2\nu\left(1 - \frac{1}{2}\nu\right)\left(\frac{1}{r} + \frac{1}{s}\right)}} = \frac{\hat{\kappa} - \hat{\omega}}{\sqrt{2\hat{\nu}\left(1 - \frac{1}{2}\hat{\nu}\right)\left(\frac{1}{r} + \frac{1}{s}\right)}}, \tag{3}$$

a standard normal distribution according to Fact 1. So correspondingly, the difference e after scaling (denoted by z) is an outcome of Z. Then an equivalent test can be made by rejecting H_0 if $z > z_\alpha$ where $z_\alpha \in \mathbb{R}$ such that $Pr[Z > z_\alpha] = \alpha$. The table listing the value of z_α as a function of α can be found in Reference[26]. Therefore, we amend the original EKSQPC protocol as follows:

Protocol 3 (REKSQPC) :

RC1 (Estimation of ω) Alice and Bob execute MRAD s times. Alice sends s qubits to Bob. He reflects all of them. In other words, there are s probing bits and zero data bits. In Step C5, Alice counts the number of PMs (denoted by $C_\rho^{'}$). Finally, she uses Equation (2) *to estimate ω. Note that during the estimation process, we need to guarantee that Eve does not perpetrate attacks.*

RC2 Alice and Bob start the execution of the protocol. They do Steps C1–C4.

RC3 In C5, instead of terminating the protocol when $p_k = 0$ and function $AE(e_{1k}, e_{2k}, i_k) = 1$, Alice increments a counter C_ρ (initial value is zero) and continues to check the remaining bits of $\underline{P}$. After finishing checking, she uses Equation (1) *to estimate κ. She tests the null hypothesis H_0: $\kappa = \omega$ against the alternative hypothesis H_1: $\kappa > \omega$,* Equation (3). *If H_0 is rejected, Alice considers the protocol is insecure and terminates it; otherwise, Alice and Bob execute Steps C6 and C7 to complete the data transmission.*

When ω is given, Alice can simply compare it with the estimation of κ. Similarly, we need to test H_0: $\kappa = \omega$ against H_1: $\kappa > \omega$. Since ω is not estimated but a given constant, we can say $\hat{\omega} \sim N(\omega, 0)$. We estimate the real attack rate κ by Equation (1). Applying Fact 3, we have that $E = \hat{\kappa} - \omega = \hat{\kappa} - \hat{\omega} \sim N\left(\kappa - \omega, \frac{2\kappa\left(1-\frac{\kappa}{2}\right)}{r}\right)$. Under the assumption that H_0 is true, $E \sim N\left(0, \frac{2\kappa\left(1-\frac{\kappa}{2}\right)}{r}\right)$. Applying Fact 1, we scale E to $Z' = \frac{(\hat{\kappa} - \omega) - 0}{\sqrt{\frac{2\kappa\left(1-\frac{\kappa}{2}\right)}{r}}} = \frac{\hat{\kappa} - \omega}{\sqrt{\frac{2\kappa\left(1-\frac{\kappa}{2}\right)}{r}}} \sim N(0, 1)$. Let z' denote

the scaled difference of the estimated κ and the pre-known ω, which is an outcome of Z'. We reject H_0 if $z' > z_\alpha$, where the definition of z_α is unchanged.

Since ω is given, its estimation is unnecessary. To complete the data transmission, Alice and Bob only need to implement Steps RC2 and RC3, where Z is replaced by Z'.

Security analysis of REKSQPC. As we have mentioned at the beginning of this section, the original MRAD fails if the qubits transmitted are disturbed and the entanglement is destroyed. The false positives mislead the protocol about the transmission security and cause wrong termination. To fix the problem, in Sections 4.1, we propose a new detection method for MRA based on a statistical test. The method detects the discrepancy between ω and κ, which does not exist if there is no attack. If any significant discrepancy is identified, the protocol is considered insecure and terminated.

The test rules out the possible outcomes of E that are largely greater than zero, and thus, introduces detection errors. In more details, suppose that Eve does not perpetrate attacks, which implies $\kappa = \omega$ and the null hypothesis H_0 is true. Due to the fluctuation of the estimator D, the difference between $\hat{\kappa}$ and $\hat{\omega}$, there is a probability α that the sampling of D is greater than the threshold d_α and gets the H_0 rejected, which is a false positive. Correspondingly, if Eve perpetrates attacks and causes $\kappa > \omega$, it is also possible that H_0 is not rejected since their difference is still less than d_α, which is a false negative. We formally define these two types of errors as follows,

Definition 4 (Type A Error - False Negative). *Eve perpetrates an attack, but the protocol is wrongly considered secure.*

Definition 5 (Type B Error - False Positive). *Eve does not perpetrate an attack, but the protocol is wrongly considered insecure.*

The Type A Error has more adverse consequences than the Type B Error because Eve can eavesdrop the message without the awareness of Alice and Bob. We show that the probability of undetected eavesdropping is very low, even when a small number of probing bits is used. The Type B error does not undermine the security of the protocol. Instead, it lowers the transmission efficiency. While Eve does not perpetrate an attack, the Type B error causes a wrong belief of its presence and a termination of the protocol. The protocol needs to restart and resend all qubits. The transmission efficiency is affected.

The choice of a specific value for α, the occurrence probability of the Type B Error, affects the one of the Type A Error. In particular, an increase of α pushes the value of d_α to zero. Although Eve only attacks a few portion of the probing bits, the difference between κ and ω she introduces may still exceed the lowered d_α and get H_0 rejected; therefore, the test becomes stricter and the occurrence probability of Type A Error decreases. Similarly, we can show that a decrease of α leads to an increase of Type A Error occurrence probability. Since the Type A and B Error occurrence probabilities have a negative relationship, if we increase α to enhance the security level, we get more Type B Errors and lower transmission efficiency. Conversely, to decrease the overhead, security is undermined.

With the results of simulations, Fig. 4 plots the rates of the two types of errors as a function of α. For estimating the Type A Error occurrence probability, we set the probability p for Eve to attack a qubit to 10% for both cases, and the number of probing bits to estimate κ and ω (if unknown) to 600. Note that the configuration here is intended to make the Type A Error occurrence probability more sensitive to the choice of alpha, which is not typical in practical problems. We will talk about how the error occurrence probabilities behave with more common configurations in the sequel. Whether the value ω is known or not, the trends for both types are consistent with our analysis. When ω is given, the probability of the Type A Error is lower because the estimation of ω introduces more variance, which further amplifies the fluctuation of the estimation of the difference $D = \kappa - \omega$. Regarding the Type B Error, we can observe that the rate roughly equals α which makes sense since it is an estimation of it.

Besides the occurrence probability α of the Type B Error, the numbers of probing bits required to estimate ω and κ are also related to the transmission efficiency. A larger number of probing bits contributes to a better estimation, but also has higher overhead. With the results of simulations, Figs 5 and 6 plot the rates of the Type A and B Errors as a function of the number of probing bits and the attack rate. The probability ($\omega = 0.05$) that a qubits is disturbed is unknown in Fig. 5 but pre-known in Fig. 6. α is set to 0.05. In Fig. 5, the numbers of probing bits coincide for the estimation of ω and κ.

The two figures show that when Eve is more likely to attack a qubit, the detection success rate increases. If Eve only attacks a small proportion of qubits, her attacks do not significantly increase κ and thus are concealed by ω. However, in order to successfully eavesdrop messages, Eve should perpetrates attacks at a rate higher than 50%. When the probability of attacks is 60%, 60 probing bits are sufficient to avoid the Type A Error (when ω is unknown). If ω is given, then 40 probing bits can achieve the same security level.

Note that the Type B Error rate should be constant. In particular, its mean is theoretically equal to 5% as it is an estimation of α. However, while the estimated rate roughly stays around 5% in Fig. 6, a relatively considerable increase is observed in Fig. 5. The increase is due to a low number of probing bits. According to Remark 9, a good normal approximation requires a large sample size and to estimate both ω and κ, a even larger one is needed. Although, the approximation is not quite accurate when the probing bit number is small, a low level of Type A Error rate shows that it is good enough to secure the protocol.

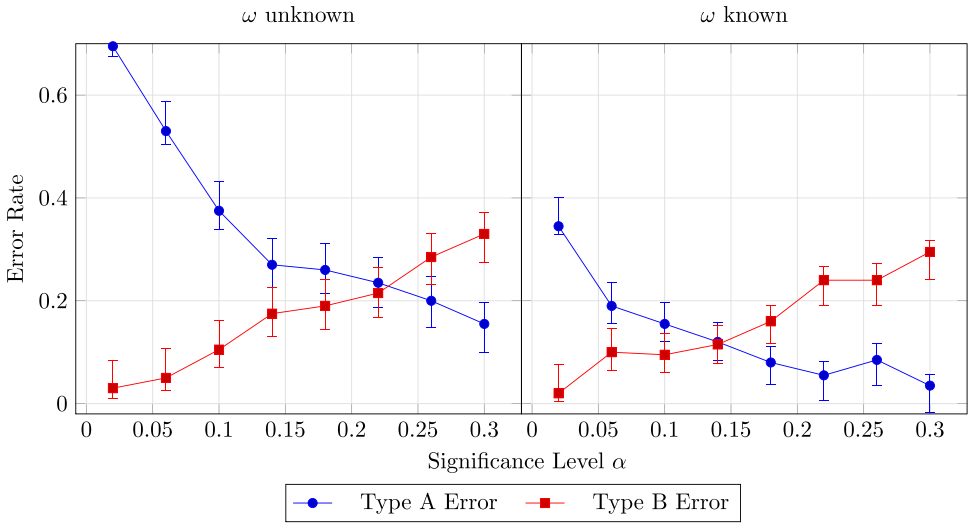

Figure 4. Error rates and their 95% confidence intervals as a function of significance level when the probability ω that a qubits is disturbed is unknown (left) and known (right). (Simulation configuration: $r = 600, s = 600$ (if ω is unknown), $\omega = 0.3, p = 0.1$).

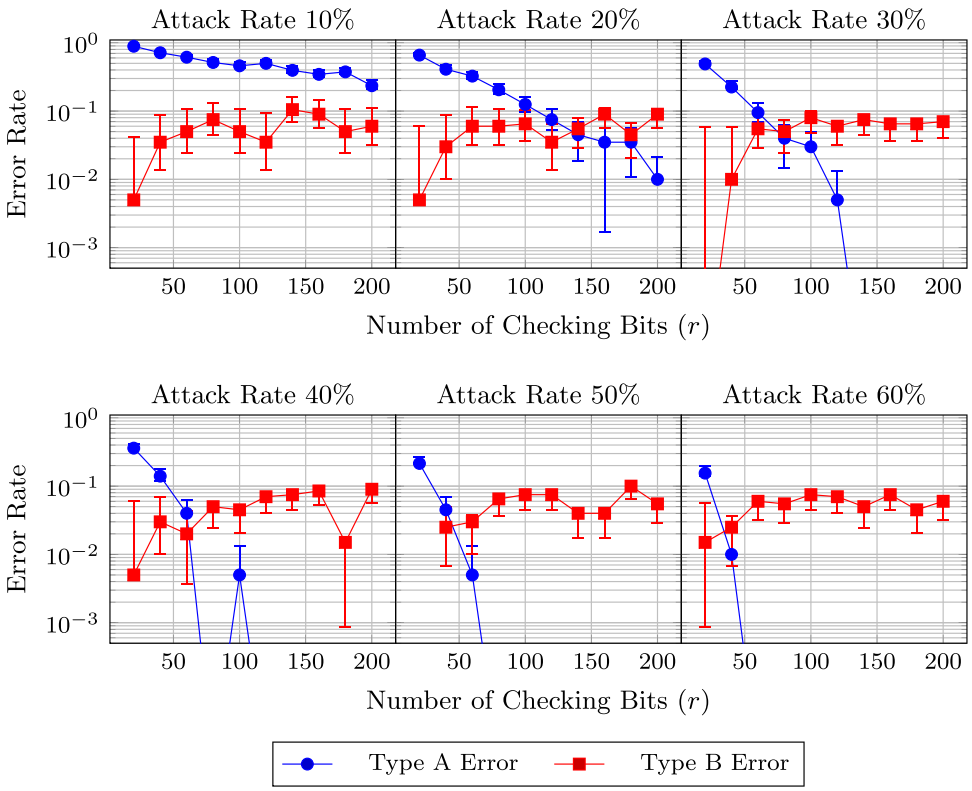

Figure 5. Error rates and their 95% confidence intervals with respect to the number of probing bits when Eve has probability $p = 0.1, 0.2, \ldots, 0.6$ to attack a qubit. (The probability ω that a qubit is disturbed is unknown. Simulation configuration: $\omega = 0.05, \alpha = 0.05$).

Since the REKSQPC and EKSQPC protocols are the same except for the part that detects MRA, Theorem 4 is also applicable to REKSQPC. In particular, we have Theorem 7.

Theorem 7. *With a sufficient number of probing bits, the Type A Error can be avoided. So the REKSQPC protocol is secure.*

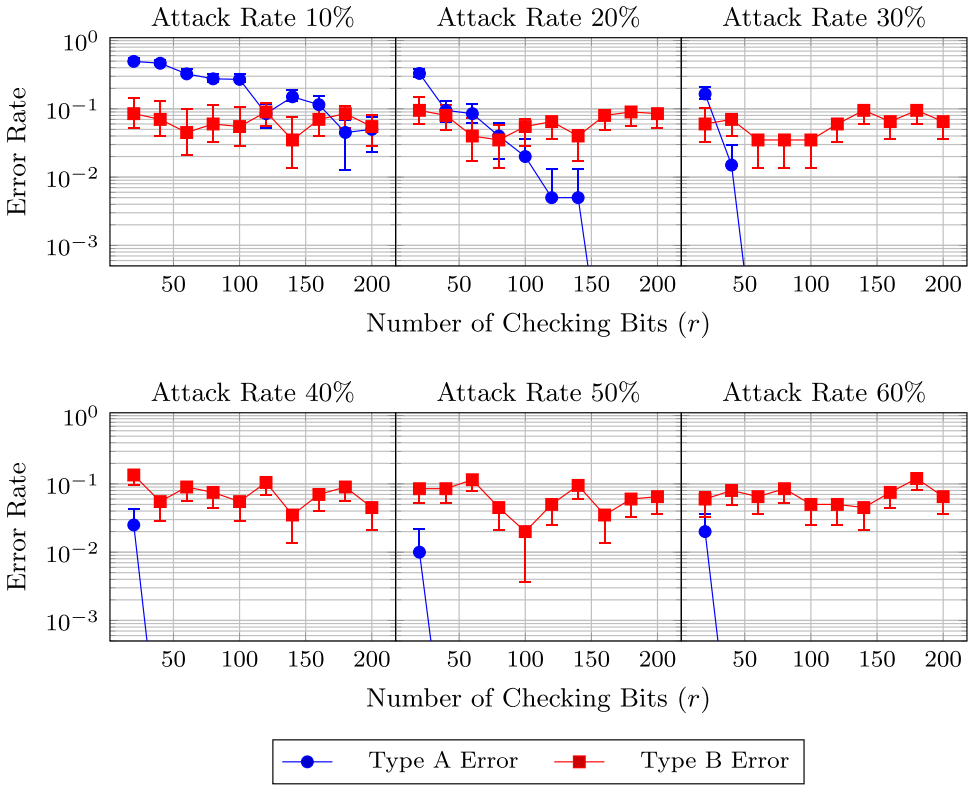

Figure 6. Error rates and their 95% confidence intervals with respect to the number of probing bits when Eve has probability $p = 0.1, 0.2, \ldots, 0.6$ to attack a qubit. (The probability ω that a qubit is disturbed is known. Simulation configuration: $\omega = 0.05, \alpha = 0.05$).

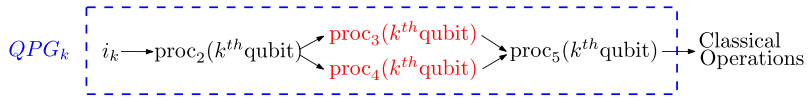

Figure 7. The EKSQPC protocol flow diagram of the procedures requiring quantum resources. *The procedures marked in red belong to Bob. For each QPG$_k$, Bob chooses either proc$_3$(k^{th} qubit)* to measure or *proc$_4$(k^{th} qubit)* to reflect.

Quantum Resource Requirements and Transmission Efficiency

In this section, we analyze the requirements of quantum resources, qubit efficiency and quantum circuit complexity of the EKSQPC protocol. Among all SQKD and SQDC protocols, we show that the EKSQPC protocol has the highest qubits efficiency (almost 100%) with the simplest quantum circuits (without qubits permutation and measurement basis switch). Comparing to the protocols utilizing the quantum entanglements, we show that the EKSQPC protocol reaches the theoretical minimum of the quregister size and the EPT among the SQKD and SQDC protocols.

Quantum resources requirements. We briefly discuss the quantum resources requirements at the end of Section 3.2. In this section, we elaborate them. Since the revised version introduced in Section 4 does not change the hardware requirements, we discuss them together.

Alice and Bob loop over i_k in I to accomplish all the operations requiring quantum resources. Hence, the lowest quantum resources requirements of the protocol implementation agrees with the one to execute a single quantum procedure group QPG_k (plotted in Fig. 7).

In order to generate EPR pairs in Procedure 2, Alice is required to have an EPR pair generation circuit. Besides, a one-bit quregister is needed to retain the first qubit of the pair. Alice needs a Bell measurement circuit to perform Procedure 5. The entanglement of the EPR pair must be preserved until Alice applies a Bell measurement on it (this case happens when the second qubits γ_B is reflected by Bob. Otherwise, Bob measures it, and the preservation time is shorter). Let C denote the time that Alice generates, sends and receives the qubits, and T the one-way time for the qubits to move between Alice and Bob. Then the EPT is $C+2T$ if we do not count the qubits reflection time of Bob. Compared to Alice, the quantum capability of Bob is fundamental. In particular, he should be able to either measure a qubit in the Z-basis, followed by sending a pre-generated $|0\rangle$, or reflect it. Overall, Alice and Bob need the following minimum quantum capabilities for the protocol implementation.

Protocols (The protocols using entanglements are marked by *)	Qubit permutation	Basis Switch	Qubit Efficiency η	Minimum# quregisters	EPT
Boyer (2009) Randomization-Based SQKD[7]	Yes	Yes	<12.5%	$4n$	0
Boyer (2009) Measure-Resend SQKD[7]	No	Yes	<12.5%	0	0
Zou (2009) Protocol 5[28]	No	Yes	<12.5%	0	0
Wang (2011)[8] *	Yes	Yes	<50%	$6n$	Worse than linear
Li (2016)[9]	No	Yes	<6.25%	0	0
Luo (2016)[10] *	Yes	Yes	12.5%	$20n$	Worse than linear
EKSQPC*	No	No	≈100%	1	$C + 2T$
REKSQPC*	No	No	≈99%	1	$C + 2T$

Table 3. Comparisons among typical SQKD and SQDC protocols.

Alice: a one-bit quregister, the circuits for Bell measurement and EPR pair generation.

Bob: a device that either reflects a qubit or uses the Z-basis to measure it followed by sending a $|0\rangle$.

Among SQDC and SQKD protocols that utilize entanglements, Alice must create at least a pair of entangled qubits and send at least one of the qubits to Bob. Therefore, for containing a qubit, a one-bit quregister is necessary. For checking the potential attacks, Alice must do some quantum operations on the qubit pair consisting of the qubit she retained and the one reflected by Bob. So, the EPT is at least $C+2T$. As the EKSQPC reaches the theoretical lower bound, we conclude that,

Theorem 8. *Among SQDC and SQKD protocols that utilize entanglements, the EKSQPC protocol only requires theoretically minimal quregister size and EPT.*

Transmission efficiency. Suppose the string $\underset{\sim}{C}\,(=\underset{\sim}{U})$ shared by Alice and Bob is updated for each dialogue. In other words, prior to applying Step C6 and Step C7 to transmit data, Alice and Bob always execute Steps C1 to C5 to share a random binary string.

Consider the original EKSQPC protocol. Suppose that an s-bit message is sent to Bob from Alice, and for each qubit Eve has probability p to perpetrate an MRA. Then, for a high eavesdropping efficiency, Eve has to choose a p close to one. Assume $p = 0.6$ and the number of probing bits is 15. Theorem 3 shows that the success rate of detection is higher than 0.995. Moreover, adding a few more probing bits can enhance the security level significantly. In practice, the message length s should considerably exceed 15. Then the probing bits can only introduce a negligible overhead. So for sending a message of length s, Alice sends roughly s qubits to Bob. Thus, the qubit efficiency approaches 100%.

If we consider the possibility that a qubit is disturbed during the qubit transmission, we need to apply the rate estimation version of the protocol. If ω is unknown, we need around 60 probing bits to reach 99% detection success rate (assuming that $\alpha = 0.01$, $\omega = 0.05$), which is acceptable considering a much larger total number of qubits transmitted. If the rate is given, then the probing bit number can decrease to 30 (extra 20 probing bits can improve the success rate to almost 100%). Then the overhead from the probing bits is negligible. The major part of the overhead is from α, the probability to get Type B Error, which causes a full restart of the protocol. In average, $\alpha \cdot 100\%$ qubits transmitted are discarded due to the wrong conclusion that the protocol is insecure. If we choose $\alpha = 0.01$ (which is big enough to secure the protocol), the overhead is only 1%.

Notice that Alice is only required to perform Bell measurements. So she only needs a fixed circuit without measurement basis switch capability. Additionally, the operations related to one qubit is irrelevant to those concerned with the others (since the message security does not depend on the bit permutation by Alice and Bob). Therefore, if the transmission or measurement of a single qubit fails, Alice and Bob only need to re-implement the operations associated with that qubit. This enhances the success rate and efficiency of the data transmission potentially.

In Table 3, we make a detailed comparison with other typical SQKD and SQDC protocols. Note that the qubit efficiency (η) is calculated by

$$\eta = \frac{\text{Length of the message}}{\text{Number of qubits sent by Alice}}.$$

For the protocols in References[7–9,28], η depends on some parameters other than the length of the message. For these protocols, we give an upper bound for η. Regarding REKSQPC, η is calculated by choosing $\alpha = 0.01$. Besides, in the protocol proposed by Li *et al.*[9], the measurement basis switch is not required of Alice or Bob but delegated to a third full quantum capability computer Charlie.

Conclusion

In this paper, we proposed a new SQDC protocol (named Economic Keyless Semi-Quantum Point-to-Point Communication). Compared to other SQDC and SQKD protocols, our new protocol has much higher qubit efficiency (almost 100%) and simpler quantum circuits (not requiring switching measurement basis or permuting qubits). While other SQKD and SQDC protocols encrypting messages through entanglements require at least linear EPT and linear size quregister, in our protocol, only Alice is required to have a fixed size (as low as one)

quregister and preserve an EPR pair entanglement for time $C + 2T$, where C is the time that Alice prepares, receives and measures the qubits, and T is the one for the qubits to move between Alice and Bob.

Among the protocols using quantum entanglements to encrypt messages, we show that both quregister size and EPT achieve the theoretical minimums. A pre-shared key is not required by our new protocol. Instead, Alice and Bob use the qubits entanglement to share a random string and further use it as a key to secure the data transmission. We used the probing bits to implement MRAD so that the protocol is resistant to MRA.

In our original protocol, Theorem 3 shows that 15 probing bits can lead to a 0.995 success rate of attack detection (given that the adversary Eve has the probability 0.6 of perpetrating an MRA on a single qubit). A few more bits can boost the security level of the protocol significantly (for example, 0.9992 detection success rate can be achieved by using 20 probing bits). If the message size is sufficiently long, then the qubit efficiency can reach almost 100%.

The rate estimation version, the protocol REKSQPC, can function properly and correctly detect attacks perpetrated by Eve while the qubits may be disturbed during the transmission. We designed a test to monitor the difference of κ, the probability that a qubit is disturbed or attacked, and ω (estimated or pre-known), the probability that a qubit is disturbed. If the difference is significantly large, the protocol terminates. The simulation results show that 60 probing bits can push detection success rate to almost 100% (assuming that $\alpha = 0.05$ and $\omega = 0.05$) if ω is unknown. The number of probing bits can decrease to 40 and achieve the same success rate if ω is pre-known. Assuming that we can always detect MRA, our protocol is secure against network attacks (Theorems 4 and 7).

References

1. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
2. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
3. Long, G. L. & Liu, X. S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **65**, 032302 (2002).
4. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050–2056 (1999).
5. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing* **26**, 1484–1509 (1997).
6. Boyer, M., Kenigsberg, D. & Mor, T. Quantum key distribution with classical bob. *Phys. Rev. Lett.* **99**, 140501 (2007).
7. Boyer, M., Gelles, R., Kenigsberg, D. & Mor, T. Semiquantum key distribution. *Phys. Rev. A* **79**, 032341 (2009).
8. Jian, W., Sheng, Z., Quan, Z. & Chao-Jing, T. Semiquantum key distribution using entangled states. *Chinese Physics Letters* **28**, 100301 (2011).
9. Li, Q., Chan, W. H. &Zhang, S. Semiquantum key distribution with secure delegated quantum computation. *Scientific Reports* **6** (2016).
10. Luo, Y.-P. & Hwang, T. Authenticated semi-quantum direct communication protocols using bell states. *Quantum Inf. Process.* **15**, 947–958 (2016).
11. Almousa, S. & Barbeau, M. Delay and reflection attacks in authenticated semi-quantum direct communications. *2016 IEEE Globecom Workshops* (*GC Wkshps*) 1–7 (2016).
12. Shukla, C., Thapliyal, K. & Pathak, A. Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. *Quantum Information Processing* **16**, 295 (2017).
13. Zhang, W. *et al*. Quantum secure direct communication with quantum memory. *Phys. Rev. Lett.* **118**, 220501 (2017).
14. Wu, F. *et al*. High-capacity quantum secure direct communication with two-photon six-qubit hyperentangled states. *Science China Physics, Mechanics & Astronomy* **60**, 120313 (2017).
15. Gu, J., Lin, P.-H. & Hwang, T. Double c-not attack and counterattack on 'three-step semi-quantum secure direct communication protocol'. *Quantum Information Processing* **17**, 182 (2018).
16. Zhong, M. *et al*. Optically addressable nuclear spins in a solid with a six-hour coherence time. *Nature* **517**, 177–180 (2015).
17. Inagaki, T., Matsuda, N., Tadanaga, O., Asobe, M. & Takesue, H. Entanglement distribution over 300 km of fiber. *Opt. Express* 23241–23249.
18. Neumann, P. *et al*. Quantum register based on coupled electron spins in a room-temperature solid. *Nat Phys* **6**, 249–253 (2010).
19. Dai, H.-N. *et al*. Generation and detection of atomic spin entanglement in optical lattices. *Nat Phys* **12**, 783–787 (2016).
20. Lu, H., Barbeau, M. &Nayak, A. Economic no-key semi-quantum direct communication protocol. In *2017 IEEE Globecom Workshops* (*GC Wkshps*), 1–7 (2017).
21. Malladi, S., Alves-Foss, J. &Heckendorn, R. B. On preventing replay attacks on security protocols. *In Proc. Int. Conf. on Security and Management* 77–83 (2002).
22. Scarani, V., Acín, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92**, 057901 (2004).
23. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
24. Kalashnikov, D. A., Tan, S. H., Chekhova, M. V. & Krivitsky, L. A. Accessing photon bunching with a photon number resolving multi-pixel detector. *Opt. Express* **19**, 9352–9363 (2011).
25. Zhou, Z. *et al*. Superconducting series nanowire detector counting up to twelve photons. *Opt. Express* **22**, 3475–3489 (2014).
26. Hogg, R., Tanis, E. &Zimmerman, D. *Probability and Statistical Inference*, 192 (Pearson Education, 2014).
27. DasGupta, A. *Normal Approximations and the Central Limit Theorem* (pp. 213–242. Springer New York, New York, NY, 2010).
28. Zou, X., Qiu, D., Li, L., Wu, L. & Li, L. Semiquantum-key distribution using less than four quantum states. *Phys. Rev. A* **79**, 052312 (2009).

Author Contributions

H.L. devised the protocol. H.L. and M.B. wrote the main manuscript, and A.N. gave solid suggestions on the manuscript. All authors reviewed the manuscript.

Additional Information

Supplementary information accompanies this paper at https://doi.org/10.1038/s41598-018-37045-0.

Competing Interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.


Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/.

© The Author(s) 2019